2) файлы БД — это файлы определенной структуры. Пользователи могут иметь доступ к информации только из определенных частей БД, то есть возникает задача ранжирования прав доступа (избирательной защиты) внутри файла БД.

3) размер шифруемой информации в файле БД в общем случае произволен и ограничен только структурой БД.

Для более полной защиты необходимо ввести следующие уровни:

1) регистрация и аутентификация пользователей, ведение системного журнала. В системном журнале регистрируются любые попытки входа в систему и все действия оператора в системе.

2) определение прав доступа к информации БД для конкретного пользователя (авторизация пользователя) при обращении к СУБД. Все действия пользователя протоколируются в системном журнале. Определение полномочий пользователя при доступе к БД происходит на основе анализа специальной информации — списка пользователей с правами доступа, которая формируется администратором БД, исходя из принципа минимальных полномочий для каждого пользователя.

3) непосредственный доступ к БД. На этом уровне для повышения защищенности системы в целом целесообразно использовать шифрование/расшифрование отдельных объектов БД. Ключи для шифрования можно определять исходя из идентификатора пользователя и его полномочий, то есть «паспорта» пользователя.

В качестве примера можно привести алгоритм, реализованный в программном средстве «Экспресс-диагностика психофизических показателей»

При создании базы данных вводится дополнительное поле, в котором записывается уровень конфиденциальности данной записи. Информация БД шифруется и хранится на диске в зашифрованном виде. В каталоге СУБД создается БД, представляющая из себя регистрационную книгу, где содержится следующая информация: имя или код пользователя, пароль, уровень доступа.

Данный файл и управляющая *.prg-программа также шифруются. Создается и запускается управляющий *.bat-файл. К недостаткам данной реализации относятся:

– возможность удаления и модификации *.bat-файла;

– при некорректном завершении (например, ctrl+a1t+del) на диске может остаться файл базы данных в явном виде.

В заключение следует отметить, что при разработке механизмов защиты БД следует помнить о некоторых их особенностях:

– в БД объекты могут представлять собой сложные логические структуры, определенное множество которых может отображаться на одни и те же физические объекты;

– возможно существование различных требований по защите для разных уровней рассмотрения — внутреннего, концептуального и внешнего для БД; защита БД связана с семантикой данных, а не с их физическими характеристиками.

Литература

1. *Риккарди Г.* Системы баз данных. Теория и практика использования в Internet и среде Java : пер. с англ. М., 2001.

2. *Роб П., Коронел К.* Системы баз данных: проектирование, реализация и управление: пер. с англ. СПб., 2004.

ПРОГРАММНЫЙ МЕТОД ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ «ЭКСПРЕСС-ДИАГНОСТИКА ПСИХОФИЗИЧЕСКИХ ПОКАЗАТЕЛЕЙ»

Н.Л. БОБРОВА

Защита программного обеспечения на сегодняшний день является одной из актуальных задач. Впервые задача защиты была озвучена в 70-х годах.

Задача защиты программного обеспечения от копирования заключается в установлении зависимости между программным обеспечением и объектом привязки. Причем объект привязки должен быть таким, который невозможно скопировать. Таким образом, скопированное защищенное программное обеспечение становиться неработоспособным в отсутствии объекта привязки.

Задача защиты программного обеспечения от копирования разбивается на две подзадачи:

1) установление зависимости между защищаемым программным обеспечением и объектом привязки;

2) создание не копируемого объекта привязки.

От того, как будут эффективно решены эти две подзадачи, зависит эффективность защиты программного обеспечения от копирования. В настоящее время для защиты программного обеспечения от копирования используются программные и аппаратно-программные методы, в которых решены обе указанные задачи.

Выбирая средство защиты, разработчик должен исходить из принципа экономической целесообразности. Защита должна выполнить свое основное предназначение — существенно сократить, а в идеале — прекратить, потери от пиратства, не сильно при этом увеличивая стоимость программы. В данной работе рассматривается защита программного обеспечения привязкой к ресурсам персонального компьютера.

Программные методы защиты программного обеспечения от копирования свободны от указанных недостатков, но по своей эффективности защищенности уступают аппаратно-программным методам. В широком смысле слова можно сказать, что программные методы уступают только аппаратно-программным, основанным на использовании USB-ключей. Так как закрыт доступ расположенному в USB ключе защищенному алгоритму приложения.

В существующих распространенных программных методах защиты программного обеспечения от копирования, задача создания не копируемого объекта привязки решена в виде использования серийных номеров оборудования компьютера [1]. А задача установки защиты решена в виде проверки серийных номеров оборудования компьютера в алгоритмах защищаемого программного обеспечения. Очевиден недостаток такого способа решения задачи защиты от копирования. Программное обеспечение, защищенное данным способом, зависимо от аппаратной конфигурации компьютера. В случае смены или изменения аппаратной конфигурации компьютера, установленное ранее защищенное программное обеспечение становиться неработоспособным.

Данный метод защиты применяется при Post-RTM (post-release to manufacturing — издание продукта, у которого есть несколько отличий от RTM и помечается как самая первая стадия разработки следующего продукта) программного обеспечения «Экспресс-диагностика психофизических показателей».

В качестве уникальных параметров персонального компьютера предлагается использовать серийный номер видеоадаптера, материнской платы. Данные параметры присваиваются устройствам на этапе их изготовления и не меняются в процессе их функционирования. Для извлечения этих параметров требуется создать специальный драйвер, которым должны комплектоваться программный продукт и программа-регистратор. Однако существует более простые способы получения уникальных характеристик персонального компьютера:

С помощью программ тестов-информаторов Sisoft Sandra, PC Wizard, Everest, дающих не только полнейшую информацию о «железе», но способных протестировать и проанализировать его работу.

Утилитой dxdiag.exe (средство диагностики DirectX от Microsoft), запущенной из «Командной строки».

С помощью программы System Info (sysinfo.exe) из пакета Norton Utilities «Информация о системе». Программа System Information дает детальную информацию об аппаратных и

программных системах, установленных на компьютере, а также вычисляет три характеристики производительности системы.

С помощью утилиты msinfo32.exe — сведения о системе.

Используемый нами метод привязки программного обеспечения пользователя к характеристикам персонального компьютера работает следующим образом:

Программный продукт:

1) анализирует параметры оборудования;

2) анализирует лицензионную информацию;

3) при несоответствии принимает меры ограничения (программа не запускается).

Модуль-регистратор:

1) анализирует параметры оборудования;

2) генерирует регистрационный ключ;

3) передает ключ пользователю продукта.

Простая реализация метода защиты программного обеспечения привязкой к параметрам персонального компьютера [2] сводит анализ лицензионной информации, сгенерированной модулем-регистратором к ее сравнению с необходимой, полученной в результате анализа параметров реального оборудования программным продуктом. Нейтрализация защиты в данном случае сводится к поиску и замене инструкции сравнения на безусловный переход.

Надежность защиты может быть увеличена путем использования криптозащиты. Шифрование должно применяться совместно с защитой от статического и динамического анализа кода программы и «изощренным программированием», т.е. стилем, позволяющим получить сложный и запутанный исполняемый модуль [3].

В программных и аппаратно-программных методах основанных на привязке защищаемого программного обеспечения к его непосредственному носителю возникает дополнительная задача. Эта задача заключается в сокрытие от злоумышленника алгоритмов защищенного программного обеспечения, в которых реализована проверка наличия объекта привязки. Для сокрытия алгоритмов получили распространение следующие методы:

1) метод запутывания;

2) метод виртуального процессора;

3) метод мусора.

Литература

1. *Шалатонин И.А., Коваленко П.П.* Международный конгресс по информатике: информационные системы и технологии: материалы международного научного конгресса 31 окт. – 3 нояб. 2011 г. : в 2 ч. Ч. 2. Минск: БГУ, 2011. С. 146–150.

2. *Хорев П.Б.* Методы и средства защиты информации в компьютерных системах. М., 2005.

3. *Абашеев А.А., Жуков И.Ю., Иванов М.А. и др.* Ассемблер в задачах защиты информации. М., 2004.

МЕТОД БЛОЧНОГО МАРКИРОВАНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ СИНУСОИДАЛЬНЫХ РЕШЕТОК

А.А. БОРИСКЕВИЧ, Ю.А. КОЧЕТКОВ

Традиционные двумерные штрих-коды (QR-коды) не несут визуальной информации и ограничены по информационной емкости.

В связи с этим предложен метод блочного маркирования изображений и оптоэлектронного извлечения сообщения, основанный на внесение избыточности в информационное бинарное сообщение и его зашифровании, генерации двумерных синусоидальных решеток с различными идентификационными параметрами (частота, ориентация, размер) для кодирования информационного сообщения, перцептуальном гибридном внедрении маркирующей синусоидальной маски, формирование контура обнаружения маркируемого изображения, обнаружение контура для оптического захвата